Matthew Q. Wetherington
Adam L. Hoipkemier
THE WERNER LAW FIRM
2142 Vista Dale Court
Atlanta, GA 30084
Phone: (770) VERDICT
matt@wernerlaw.com
adam@wernerlaw.com

Shireen Hormozdi
HORMOZDI LAW FIRM, LLC
1770 Indian Trail Lilburn Road
Suite 175
Norcross, GA 30093
Phone: 800-994-9855
shireen@norcrosslawfirm.com

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF NORTH CAROLINA

IVAN WU, PATRICK JOHNSON, and	)	
MICHAEL REINERT, individually and	)	Civil Action No.
on behalf of all others similarly situated,	)	5:15-cv-108
	)	
Plaintiff,	)	
	)	
v.	)	
	)	
LENOVO (UNITED STATES), INC. and	)	
SUPERFISH INC.,	)	
	)	PUTATIVE CLASS ACTION
Defendants.	)	DEMAND FOR JURY TRIAL

CLASS ACTION COMPLAINT FOR DAMAGES

Plaintiffs Ivan Wu, Patrick Johnson, and Michael Reinert, individually and on behalf of all others similarly situated, file this Class Action Complaint for Damages against Defendants Lenovo (United States), Inc. and Superfish Inc. Plaintiffs bring this class action to remedy Defendants' unlawful actions in connection with the marketing and sale of certain Lenovo computers containing software that monitors user activity and intercepts, decrypts, changes, and otherwise manipulates user data, in an insecure manner that exposes users to significant data security risks, for fraudulent advertising purposes without the knowledge or consent of users.

I. INTRODUCTION

1. Defendant Lenovo began distributing computers containing an undisclosed software program called Superfish Visual Discovery (the "subject software") on September 1, 2014.

2. Defendant Superfish created the subject software and supplied it to Defendant Lenovo for inclusion on the computers.

3. The intended purpose of the subject software is to monitor a victim's Internet browsing activity, remove encryption from secure website connections,

modify the code of certain websites, and obtain fraudulent referral fees from online retailers.

4. Despite Defendants' ongoing representations to the contrary, the subject software collects personally identifying information about victims and transmits the information back to Defendant Superfish.

5. The subject software also enables persons or entities other than Defendant Superfish to monitor, modify, and redirect a victim's communications with minimal effort. This creates a significant data security risk for victims, financial institutions, government agencies, and other organizations that rely on secure Internet communications.

6. Defendants did not disclose the existence of the subject software or its intended function to purchasers of the computers. In addition, Defendant Lenovo knowingly made false statements to consumers regarding the security features of the computers.

7. Plaintiffs bring this action on behalf of themselves and all others similarly situated to recover actual damages, statutory damages, punitive damages, disgorgement of profits, injunctive and other equitable relief, and attorney's fees and costs, under a variety of federal, state, and common law claims.

II. PARTIES, JURISDICTION, AND VENUE

8. Plaintiff Wu is, and all times relevant to this action was, a citizen of the United States domiciled in California. Plaintiff brings this action in an individual capacity, and in the capacity of a class representative on behalf of others similarly situated. By bringing this action in this venue, Plaintiff avails himself of the jurisdiction of this Court.

9. Plaintiff Johnson is, and all times relevant to this action was, a citizen of the United States domiciled in New Mexico. Plaintiff brings this action in an individual capacity, and in the capacity of a class representative on behalf of others similarly situated. By bringing this action in this venue, Plaintiff avails himself of the jurisdiction of this Court.

10. Plaintiff Reinert is, and all times relevant to this action was, a citizen of the United States domiciled in Pennsylvania. Plaintiff brings this action in an individual capacity, and in the capacity of a class representative on behalf of others similarly situated. By bringing this action in this venue, Plaintiff avails himself of the jurisdiction of this Court.

11. Defendant Lenovo (United States), Inc. is a Delaware corporation engaged in the design, manufacture, and sale of consumer goods, including

computers, in North Carolina and throughout the United States. Defendant's principal corporate office is located in Morrisville, North Carolina. Defendant Lenovo may and will be served with Summons and this Complaint through its registered agent for service of process in Wake County, North Carolina: CT Corporation System, 150 Fayetteville St., Box 1011 Raleigh, NC 27601.

12. Defendant Superfish is a Delaware corporation engaged in the design and distribution of computer and mobile device software in North Carolina and throughout the United States. Defendant's principal corporate office is in Palo Alto, California. Defendant Lenovo may and will be service with Summons and this Complaint through its registered agent for service of process: The Corporation Trust Company, Corporation Trust Center 1209 Orange St, Wilmington, DE 19801.

13. This court has jurisdiction over this action under the Class Action Fairness Act of 2005, 28 U.S.C. § 1332(d). The aggregate claims of the proposed classes vastly exceed $5,000,000.00, exclusive of interest and costs, there are believed to be in excess of 100 class members, and more than two-thirds of the proposed class members reside in different states than either or both Defendants.

14. This Court has subject matter jurisdiction over this action pursuant to 28 U.S.C. § 1331 because Plaintiffs allege the violation of numerous federal statutes.

15. This Court has personal jurisdiction over Defendant Lenovo because its principal office is in this District, derives substantial profits from this district, and otherwise has sufficient minimum contacts in this District to render the exercise of jurisdiction by this Court permissible under traditional notions of fair play and substantial justice.

16. This Court has personal jurisdiction over Defendant Superfish because it derives substantial profits from this district, and otherwise has sufficient minimum contacts in this District to render the exercise of jurisdiction by this Court permissible under traditional notions of fair play and substantial justice.

17. Pursuant to 28 U.S.C. § 1391, venue is proper in this District because Lenovo's headquarters is located here and Defendants conduct business in this District.

III. STATEMENT OF FACTS

A. Bloatware on Lenovo Computers

18. Defendant Lenovo is a corporation engaged in the design, manufacture, marketing, and sale of consumer goods, including computers.

19. In the United States, Defendant Lenovo distributes personal computers designed for consumer use with an operating system (usually Windows) preinstalled.

20. Through its marketing, packaging, and other channels, Defendant Lenovo discloses which operating system is preinstalled on a Lenovo computer prior to its sale.

21. Consumers are not given a choice to purchase a personal computer from Defendant Lenovo without an operating system.

22. In additional to the operating system, Defendant Lenovo also preinstalls a variety of "value-added" software titles to enhance the functionality, security, or fun of the computer.

23. Through its marketing, packaging, and other channels, Defendant Lenovo discloses which "value-added" software is preinstalled on a Lenovo computer prior to its sale.

24. Consumers are not given a choice to purchase a personal computer from Defendant Lenovo without "value-added" software preinstalled.

25. In addition to the reasonable and necessary operating system and "value-added" software preinstalled on its computers, Defendant Lenovo also solicits software companies and/or state actors to pay Defendant Lenovo for

preinstalling spyware, malware[1], and/or adware[2] software that reduces the functionality, security, and fun of the computer.

26. Through its marketing, packaging, and other channels, Defendant Lenovo does not disclose or will actively hide the existence of spyware and malware preinstalled on a Lenovo computer prior to its sale.

27. Spyware cannot be fully concealed because it disrupts the reasonable and ordinary use of a computer. In these instances, Defendant Lenovo will falsely represent that the spyware is “value-added” software.

28. Consumers are not given a choice to purchase a personal computer from Defendant Lenovo without spyware, malware, and/or adware software preinstalled.

29. Cumulatively, the preinstalled software on a Lenovo computer, other than the operating system, is called “bloatware.”

30. At some point prior to September 1, 2014, Defendants Lenovo and Superfish entered into a joint enterprise with a common purpose of preinstalling the subject software on certain computers.

[1] Malware is ‘malicious’ software used to disrupt computer operation, gather sensitive information, or gain access to private computer systems.

[2] Adware is software used to display advertisements without the consent of a user. Unlike advertising-supported software, most adware is difficult to disable or uninstall.

31. Upon information and belief, on or near September 1, 2014, Defendant Lenovo began distributing some or all the following computers with the subject software preinstalled (the “subject computers”):

E-Series	E10-30
Flex-Series	Flex2 14, Flex2 15, Flex2 14D, Flex2 15D, Flex2 Pro, Flex 10
G-Series	G410, G510, G710, G40-30, G40-45, G40-70, G40-80, G50-50, G50-45, G50-70, G50-80, G50-80Touch
Edge 15	all
Miix-Series	Miix2 – 8, Miix2 – 10, Miix2 – 11, Miix 3 - 1030
S-Series	S310, S410, S415, S415 Touch, S435, S20-30, S20-30 Touch, S40-70
U-Series	U330P, U430P, U330 Touch, U430 Touch, U530 Touch
Y-Series	Y430P, Y40-70, Y40-80, Y50-70, Y70-70
Yoga-Series	Yoga2-11, Yoga2-13, Yoga2Pro-13, Yoga3 Pro
Z-Series	Z40-70, Z40-75, Z50-70, Z50-75, Z70-80

B. Superfish’s Value-Added “Features”

32. The subject software is a sophisticated form of malware and adware because it masquerades as “value-added” software.

33. Defendant Superfish presents itself as a company focused on visual search.

34. Visual search, as opposed to textual search, maps relationships and similarities between images. Visual search finds results without the need for keywords or other meta data identifying the image. For example, visual search is used to recognize a human face and identify that person in other photos or environments.

35. Defendant Superfish has focused its visual search efforts in the field of matching product images on retailer websites.[3]

36. Under ideal circumstances, the subject software can recognize a product image on a retailer's website and then find the same or similar images on competing retailer websites. This enables a visual searcher to compare prices between retailers.

C. Superfish Only Exists as Bloatware

37. Unlike normal visual search engines, like tineye.com or Google Image Search, Defendant Superfish does not offer a website where a user can provide a image and find matching results.

[3] Recently, Defendant Superfish has expanded its efforts to include software that recognizes flowers or dogs.

38. In 2009, Defendant Superfish offered its technology in the form of a browser toolbar.[4] Instead, Superfish pays other companies to bury Superfish's programs in their products.

39. The subject software and its predecessors, like Window Shopper, are buried in a variety of browser toolbars, computer programs, and even antivirus programs.

40. A victim of a Superfish product installation rarely, if ever, affirmatively chooses to receive the software. Sometimes, the program is a default "add-on" that a user must identify and unselect while installing other software. More often, the victim is not told that the subject software is installed on his or her computer.

D. Superfish is Spyware

41. Similar to a keylogger, the subject software, as installed on the subject computers, monitors every Internet connection on an infected computer.

42. The subject computers utilize the Windows Filtering Platform to regulate the integrity, priority, and security of a computer's network interfaces and

[4] Knight, Christina, BizReport Advertising, *Are you ready for visual search?*, December 17, 2010, available at http://www.bizreport.com/2010/12/are-you-ready-for-visual-search.html (last accessed March 14, 2015).

connections. Every ingoing and outgoing network connection and communication must go through the Windows Filtering Program on the subject computers.

43. The subject software exploits the Windows Filtering Platform through the use of a secondary program called Komodia Redirector.

44. Komodia Redirector enables the subject software to "modify or examine all incoming and outgoing packets" without a victim knowing.[5]

45. Defendant Superfish uses Komodia Redirector to intercept and record the address of every website visited on the following web browsers: Chrome, Firefox, Internet Explorer, Maxthon, Opera, and Safari.

46. The subject software assigns a unique identification code to every installation, meaning website visits are matched to individual installations.

47. Every time a victim attempts to connect to a website, the subject software sends the victim's unique identification code, website address requested, and other information to a server owner or controlled by Defendant Superfish.

[5] Komodia, *Retail Products*, available at www.komodia.com/wfp_hl (last accessed March 15, 2015); Komodia, SSL over TCP/IP, available at http://blog.komodia.com/2008/11/ssl-over-tcpip.html (last accessed March 14, 2015).

48. The subject software harvests victim browsing information and transmits it to servers owned or controlled by Defendant Superfish, including, but not limited to, the following ip addresses:

a. 66.70.34.95;
b. 66.70.34.97;
c. 66.70.34.101;
d. 66.70.34.103;
e. 66.70.34.105;
f. 66.70.34.111;
g. 66.70.34.113;
h. 66.70.34.115;
i. 66.70.34.117;
j. 66.70.34.119;
k. 66.70.34.121;
l. 66.70.34.123;
m. 66.70.34.125;
n. 66.70.34.127;
o. 66.70.34.129;
p. 66.70.34.251;
q. 66.70.35.12; and
r. 66.70.35.48.

49. Defendant Superfish logs each connection and tracks victim's browsing history over time.[6]

[6] *See* Superfish Press Release, *Online Holiday Shoppers Prefer Sleigh Beds to iPads When Using Visual Search* (December 19, 2011), available at http://www.businesswire.com/news/home/20111219005451/en/Online-Holiday-Shoppers-Prefer-Sleigh-Beds-iPads (last accessed March February 18, 2015) (discussing Superfish's ability to track user browsing trends); *see also* Superfish Code as it existed December 15, 2014, https://www.superfish.com/ws/sf_code.jsp.

50. Defendant Superfish pays Komodia less than $0.007 for every victim subjected to the subject software.[7]

51. Under certain conditions described below, the subject software also transmits the contents (not just the address) of the web pages a victim attempts to access.

52. Defendants Lenovo and Superfish had actual knowledge of the spyware functionality of the subject software, but failed to disclose it to users and/or took affirmative steps to hide the spyware functionality of the subject software.

E. Superfish is Malware

53. In addition to spying on victims, the subject software maliciously intercepts, redirects, and changes the victim's normal and secure Internet communications.

54. Internet browser connections are generally transmitted through one of two Hypertext Transfer Protocol ("HTTP") standards: standard and secure.

55. HTTP refers to a standard Internet communication transmitted without encryption.

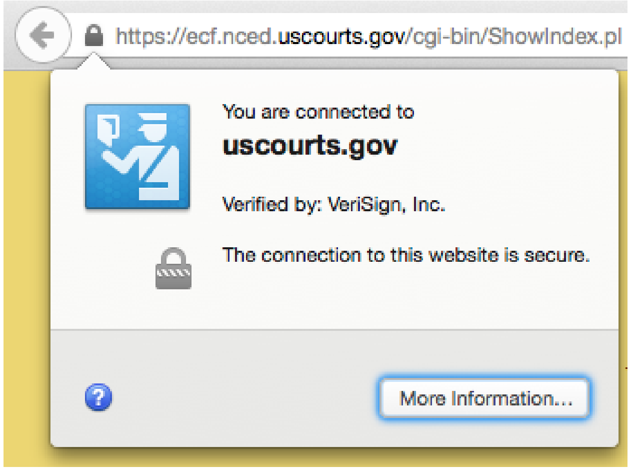
[7] Komodia, *Price* Quote, available at www.komodia.com/quotes/RedirectorQ.pdf (last accessed March 15, 2015).

56. HTTPS refers to a secure Internet communication transmitted with bidirectional encryption. HTTPS "prevents eavesdroppers from seeing the contents of your communication with a website, including potentially sensitive data such as the contents of your email and chats, login credentials, search terms, and credit card numbers."[8]

57. HTTPS-secured websites use public key certificates to ensure the security and privacy of Internet traffic between users and the website.[9] A website owner purchases a digital certificate from a certified issuer. Internet browsers automatically verify the authenticity and security of HTTPS communications by comparing the certificate provided by the website to an authoritative copy maintained by the issuing authority. Once verified, the user provides his or her own digital certificate to the website and a secure exchange of data begins.

[8] Electronic Frontier Foundation, *HTTPS*, available at https://www.eff.org/pages/https (last accessed March 10, 2015).

[9] *See* Mozilla Support, *How do I tell if my connection to a website is secure?*, available at https://support.mozilla.org/en-US/kb/how-do-i-tell-if-my-connection-is-secure?as=u&utm_source=inproduct (last accessed March 2, 2015).



https://ecf.nced.uscourts.gov/cgi-bin/ShowIndex.pl

You are connected to

uscourts.gov

Verified by: VeriSign, Inc.

The connection to this website is secure.

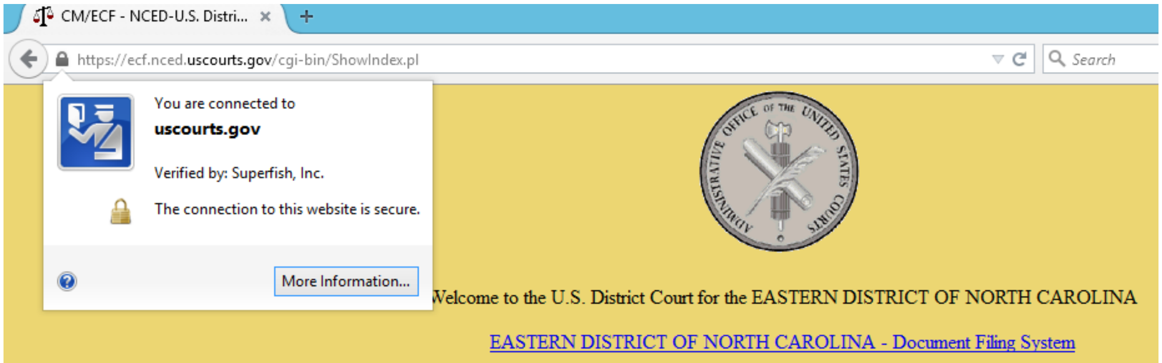
Digital certificate verification for the Eastern District of North Carolina before Superfish Infection

58. The integrity of HTTPS communications and digital certificates are critical to financial transactions, government and civilian communications, and every other routine and ordinary usage of the Internet.[10]

59. Digital certificate issuers utilize advanced cryptographic security measures to ensure that a secure communication cannot be read by anyone other than its intended recipient. These measures include serial numbers, electronic signatures, expiration dates, and thumbprints.

60. The subject software eliminates the security of digital certificates.

[10] Internet Engineering Task Force, *The Transport Layer Security (TLS) Protocol, Version 1.2*, available at http://tools.ietf.org/html/rfc5246 (last accessed March 9, 2015).


CM/ECF - NCED-U.S. Distri...

https://ecf.nced.uscourts.gov/cgi-bin/ShowIndex.pl

You are connected to **uscourts.gov**

Verified by: Superfish, Inc.

The connection to this website is secure.

Welcome to the U.S. District Court for the EASTERN DISTRICT OF NORTH CAROLINA

EASTERN DISTRICT OF NORTH CAROLINA - Document Filing System

Digital certificate verification for the Eastern District of North Carolina after Superfish Infection
This connection is NOT secure.

61. Defendants use a secondary program called Komodia SSL Decoder/Digester to carry out a "man-in-the-middle" attack on victim's secure connections.[11]

62. During the attack, both the victim and the website believe they are communicating securely with each other. Instead, both parties are communicating directly with the subject software, which acts as an intermediary between them.

63. Defendant Superfish accomplishes this attack in two steps. First, the subject software designates itself as a digital certificate issuer for the subject

[11] Graham, Robert, Errata Security, *Extracting the SuperFish Certificate*, February 19, 2015, blog.erratasec.com/2015/02/extracting-superfish-certificate.html (last accessed February 26, 2015); *see also* Komodia, *SSL Sniffing/Hijacking and SSL Decrypting SDK*, http://www.komodia.com/products/komodias-ssl-decoderdigestor/ (last accessed March 2, 2015).

computers.[12] Second, the subject software hijacks every secure communication attempted by a victim and replaces both the user's and website's real digital certificates with fake certificates created by the subject software.[13] The subject software then falsely represents itself to both parties as the intended recipient of secure communications.[14]

64. By intercepting both sides of a communication, the subject software can monitor the communications of seemingly secure HTTPS communications without detection.

65. Once a victim's encrypted communications are hijacked, the subject software continues to monitor, log, and upload user information to Defendant Superfish in the same manner that it exploits normal HTTP communications.

[12] 0xebfe, *The Analysis of SuperFish Adware*, February 20, 2015, available at www.0xebfe.net/blog/2015/02/20/the-analysis-of-superfish-adware/ (last accessed February 26, 2015).

[13] Graham, Robert, Errata Security, *Extracting the SuperFish Certificate*, February 19, 2015, available at blog.erratasec.com/2015/02/extracting-superfish-certificate.html (last accessed February 26, 2015); Graham, Robert, Errata Security, *Some Notes On SuperFish*, February 19, 2015, available at http://blog.erratasec.com/2015/02/some-notes-on-superfish.html (last accessed

[14] For an example of this attack in action, *See* Komodia, *Redirecting HTTPS Site Into Another Without Alerting User or Browser*, December 8, 2008, available at https://www.youtube.com/watch?v=MxG-B8Zcv04 (last accessed March 12, 2015).

66. Defendants' approach is "inherently one of the most potent attacks because it allows for exploitation of services that people assume to be secure."[15]

67. In addition to the harm caused by Defendants fraudulently intercepting victim's communications, the subject software also enables other parties to easily intercept and modify a victim's seemingly secure communications.

68. The subject software exposes victims to further losses and damages due to the incompetence and/or malicious intent of Defendants.

69. The subject software uses the same password for every fake digital certificate generated on a subject machine.

70. Like a several million room hotel that uses the same key for every door, the singular password used by Defendants is also the same on all of the subject computers.

71. When creating a fake digital certificate, the subject software replaces the unique 256-bit bilateral encryption normally used with a single, easy to guess, password: komodia.[16]

[15] Chris Saunders, *Understanding Man-In-The-Middle Attacks – Part 4: SSL Hijacking*, June 10, 2010, http://www.windowsecurity.com/articles-tutorials/authentication_and_encryption/Understanding-Man-in-the-Middle-Attacks-ARP-Part4.html (last accessed February 26, 2015).

72. The subject software's digital security password was cracked in just ten seconds by security researchers.[17]

73. Any third party that knows the password for the subject software can act as a second man-in-the-middle to monitor communications or even redirect victims to fake or dangerous websites. According to the United States Computer Emergency Readiness Team, "This means websites, such as banking and email, can be spoofed without a warning from the browser."[18]

74. In addition to using a trivial password, the subject software has other programming flaws.

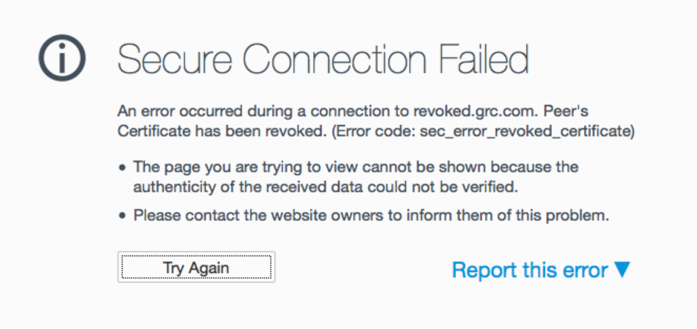
75. The subject software lacks any ability to verify that a third party certificate it is replacing was actually a valid certificate. The subject software also authenticates any security certificate received from a third party, regardless of validity, where the certificate lists the target server in the "alternative name" field of the certificate. This means the subject software affirmatively states that

[16] Graham, Robert, Errata Security, *Extracting the SuperFish Certificate*, February 19, 2015, available at blog.erratasec.com/2015/02/extracting-superfish-certificate.html (last accessed February 26, 2015).

[17] *Id.*

[18] United States Computer Emergency Readiness Team, *Alert (TA15-051A) - Lenovo Superfish Adware Vulnerable to HTTPS Spoofing*, February 24, 2015, available at https://www.us-cert.gov/ncas/alerts/TA15-051A (last accessed March 15, 2015).

fraudulent, outdated, revoked, or otherwise invalid security certificates received from third parties are valid.

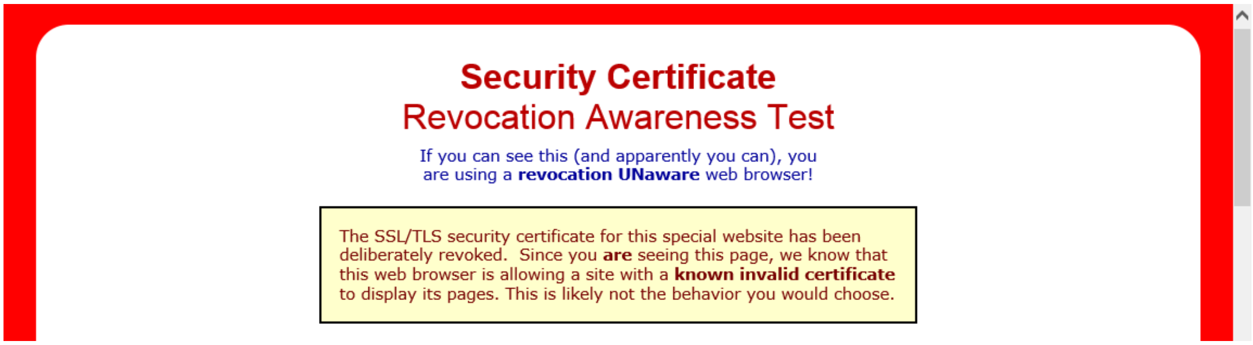


Secure Connection Failed

An error occurred during a connection to revoked.grc.com. Peer's Certificate has been revoked. (Error code: sec_error_revoked_certificate)

- The page you are trying to view cannot be shown because the authenticity of the received data could not be verified.
- Please contact the website owners to inform them of this problem.

Browser integrity test at https://revoked.grc.com/ without the subject software



Security Certificate

Revocation Awareness Test

If you can see this (and apparently you can), you are using a **revocation UNaware** web browser!

The SSL/TLS security certificate for this special website has been deliberately revoked. Since you **are** seeing this page, we know that this web browser is allowing a site with a **known invalid certificate** to display its pages. This is likely not the behavior you would choose.

Browser integrity test at https://revoked.grc.com/ with the subject software

76. During an initial investigation of the subject software, the Electronic Frontier Foundation found evidence of up to 1600 attacks by third parties using the security vulnerabilities in the subject software:

> Affected domains included sensitive websites like Google (including mail.google.com, accounts.google.com, and checkout.google.com), Yahoo (including login.yahoo.com), Bing, Windows Live Mail, Amazon, eBay (including checkout.payments.ebay.com), Twitter, Netflix, Mozilla's Add-Ons website, www.gpg4win.org, several banking websites (including mint.com and domains from HSBC and

> Wells Fargo), several insurance websites, the Decentralized SSL Observatory itself, and even superfish.com[19]

77. The Electronic Frontier Foundation's reports demonstrates that the subject software and its security flaws create a real and immediate threat of "attacks which gave attackers access to people's email, search histories, social media accounts, e-commerce accounts, bank accounts, and even the ability to install malicious software that could permanently compromise a user's browser or read their encryption keys."[20]

78. In addition to hijacking secure connections, issuing fake certificates, and exposing user data, the subject software also disrupts reasonable and ordinary usage of the subject computers by injecting a line of code into every website requested by a victim.[21]

[19] Bonneau, Joseph and Guillula, Jeremy, Electronic Frontier Foundation, *Dear Software Vendors: Please Stop Trying to Intercept Your Customers' Encrypted Traffic*, February 25, 2015, available at https://www.eff.org/deeplinks/2015/02/dear-software-vendors-please-stop-trying-intercept-your-customers-encrypted (last accessed March 10, 2015).

[20] *Id.*

[21] 0xebfe, *The Analysis of SuperFish Adware*, February 20, 2015, available at www.0xebfe.net/blog/2015/02/20/the-analysis-of-superfish-adware/ (last accessed February 26, 2015).

79. The injected code connects to a javascript file, sf_main.jsp, stored on Defendant Superfish's servers.[22]

80. The sf_main.jsp javascript file executes thousands of lines of additional code in several other JavaScript and ActionScript files.[23]

81. The code injected by the subject software reduces computer and network performance through the unauthorized use of system and networking resources on the subject computers.[24]

82. The code injected by the subject software is used to extract user information from victim's computers and transmit it to servers owned or operated by Defendant Superfish.

83. Defendants Lenovo and Superfish had actual knowledge of the malware functionality of the subject software, but failed to disclose it to users and/or took affirmative steps to hide the malware functionality of the subject software.

[22] *Id.*

[23] *See* https://www.best-deals-products.com/ws/sf_main.jsp? (last accessed March 16, 2015).

[24] *See* Mozilla Developer Network, *Tips for Authoring Fast-Loading HTML Pages*, November 2, 2014, available at https://developer.mozilla.org/en-US/docs/Web/Guide/HTML/Tips_for_authoring_fast-loading_HTML_pages (last accessed March 15, 2015).

F. Superfish is Adware

84. In addition to spying on victims and maliciously intercepting, redirecting, and changing victim's normal and secure Internet communications, the subject software also serves unwanted advertisements.

85. Using the spyware and malware functions described above, the subject software scans the text of every website a victim accesses.[25]

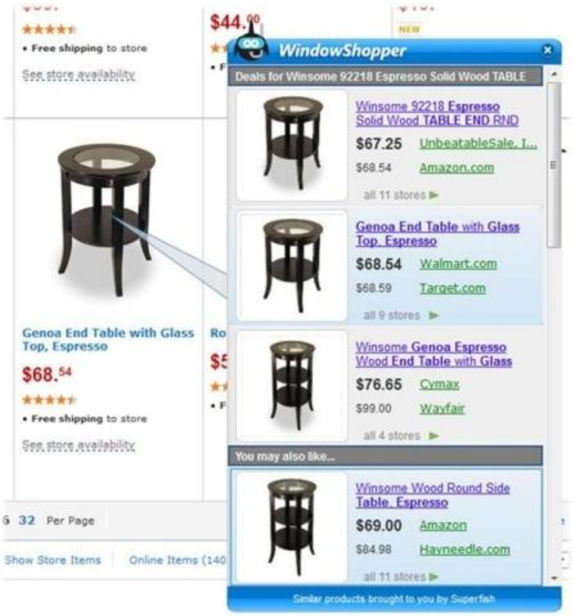
86. On certain retailer websites targeted by Defendant Superfish, the subject software will attempt to match the images in the webpage to its database of similar images.[26]

87. When a match is found, the subject software injects unexpected and non-consensual advertising into the body of the web page requested.

88. Sometimes, the subject software uses obtrusive advertising that identifies itself as presented by Defendant Superfish. Other times it does not.

[25] Knight, Christina, BizReport Advertising, *Are you ready for visual search?*, December 17, 2010, available at http://www.bizreport.com/2010/12/are-you-ready-for-visual-search.html (last accessed March 14, 2015).

[26] *Id.*



Example of advertisement from a Superfish product

89. If a victim unintentionally clicks on certain injected advertisements, Defendant Superfish makes money. According to Superfish's Director of Product, John Dew, "You will need to balance the complaints you'll inevitably receive from a few users with the revenue and added functionality benefits you get with the monetization tool you integrated."[27]

90. If the victim purchases a product from an injected advertisement, Defendant Superfish makes money based on a referral fee it extracts from the

[27] Quora, Browser Extensions and Plugins, *How Do Browser Extensions Monetize?*, August 1, 2012, available at http://www.quora.com/Browser-Extensions-and-Plugins/How-do-browser-extensions-monetize (last accessed March 13, 2015) (Plaintiffs note that eight Superfish employees, including its President, Adi Pinhas, 'liked' John Dew's statement.)

retailer.[28] In most instances, Defendant Superfish's practices violate the retailer's referral fee terms and conditions.

91. As early as September 29, 2011, Defendant Superfish had actual knowledge that its practices violate the terms of use of most browsers because it functions in a manner the user does not want or expect. When asked, "Is it okay to monetize a browser extension by inserting advertisements into some web sites?" Superfish's Director of Product, John Dew, replied, "I think the answer is maybe… there is some gray area to this." In response, a Firefox Browser contributor stated, "**The official policy is an explicit 'no'**" and referred Superfish to the Firefox terms of use.**[29]**

92. Defendants Lenovo and Superfish had actual knowledge of the spyware functionality of the subject software, but failed to disclose it to users and/or took affirmative steps to hide the spyware functionality of the subject software.

G. Defendant Lenovo's Fraudulent Marketing Practices

[28] Fox-Brewster, Thomas, Forbes, *Superfish: A History of Malware Complaints and International Surveillance*, *Forbes*, (February 19, 2015), available at http://www.forbes.com/sites/thomasbrewster/2015/02/19/superfish-history-of-malware-and-surveillance/ (last accessed February 26, 2015.)

[29] Quara, September 29, 2011, available at http://www.quora.com/Is-it-okay-to-monetize-a-browser-extension-by-inserting-advertisements-into-some-web-sites (last accessed March 13, 2015).

93. Defendant Lenovo tested and otherwise evaluated the subject software prior to installing it on the subject computers.

94. Defendant Lenovo marketed and sold the subject computers with the subject software preinstalled despite its actual knowledge of the spyware, malware, and adware characteristics of the subject software.

95. Defendant Lenovo marketed and sold the subject computers with the subject software preinstalled despite its actual knowledge of the significant data security problems created by the subject software.

96. At the time it marketed, distributed, and sold the subject computers, it was well known to Defendant Lenovo that the subject computers would be used to transfer sensitive personal and financial information through Internet browsers.

97. At the time it marketed, distributed, and sold the subject computers, it was well known to Defendant Lenovo that using a root security certificate with the same encryption key on each of the subject computers was a significant deviation from acceptable security practices and would create a significant security exposure for users.

98. At the time it marketed, distributed, and sold the subject computers, it was well known to Defendant Lenovo that its prospective and actual customers

would not consent to third-party monitoring and tracking of every website visited on the subject computers.

99. At the time it marketed, distributed, and sold the subject computers, it was well known to Defendant Lenovo that an essential purpose for using the subject computers would be to securely save and transfer sensitive personal and financial information on the Internet.

100. Defendant Lenovo concealing one or more of the following material facts regarding the subject computers and subject software to prospective and actual purchasers of the subject computers:

a. The subject software monitors and/or records user data without the knowledge or consent of users;

b. The subject software intercepts user browser data and redirects it to servers owned and/or operated by Defendant Superfish without the knowledge or consent of users;

c. The subject software transmits the browsing history of users to Superfish owned or controlled servers without the knowledge or consent of users;

d. The subject software causes internet browsers to stop responding or crash without notice;

e. The subject software blocks users from accessing websites that correctly identify the security threat posed by the subject software;

f. The subject software blocks users from directly accessing websites without connecting to servers owned and/or operated by Defendant Superfish first;

g. The subject software intercepts encrypted data users intend to send to a third-party server, decrypts the data through SSL hijacking, re-encrypts the data with an insecure root security certificate, transmits the data to servers owned and/or operated by Defendant Superfish, and then injects targeted advertising into the data that is returned to the user’s computer;

h. The subject software affirmatively states that fraudulent, outdated, revoked, or otherwise invalid security certificates received from third parties are valid;

i. The subject software authenticates any security certificate received from a third party, regardless of validity, where the certificate lists the target server in the “alternative name” field of the certificate; and/or

j. The subject software deprives users of the ability to use the laptop to securely store sensitive personal information.

101. Defendant Lenovo marketed the subject computers as not having any of the conditions described above.

102. Defendant Lenovo represented that the subject computers were reasonably free from significant data security problems.

103. Defendant Lenovo further represented that the subject computers were reasonably fit to access the Internet without exposing personal information or other sensitive data.

104. Specifically, Defendant Lenovo touted the advanced design of the subject computers created by "2000 designers and engineers focused on factors that make a difference to users."[30]

105. Defendant Lenovo marketed the subject computers as safer than other computers due to "built-in security features to help keep your data safer."[31]

106. Defendant Lenovo marketed the subject computers as being able to "ensure total security for your data and identity" with built-in software.[32]

[30] http://shop.lenovo.com/us/en/laptops/lenovo/y-series/y50/#tab-features (last accessed March 4, 2015).

[31] http://shop.lenovo.com/us/en/laptops/lenovo/yoga-laptop-series/yoga-laptop-2-pro/#tab-features (last accessed February 28, 2015).

107. While the verbiage of these representations may have varied amongst individual computer lines, the substantive message remained the same: the subject computers are reasonably fit for securely browsing the internet and Lenovo has not accepted large amounts of money to pre-install software that hijacks secure communications, steals user information, and insecurely forwards that information to unknown third parties to facilitate unwanted and unauthorized advertising.

108. Defendant Lenovo's statements regarding the quality and/or features of the subject computers were false and served to further the deceptive and fraudulent omissions described above.

H. The Named Plaintiffs' Experiences

109. Plaintiff Wu purchased a Lenovo Z40 laptop, part number 59425582, directly from Lenovo on September 27, 2014. Plaintiff Wu's computer came with the subject software pre-installed.

110. Plaintiff Wu viewed and relied on the marketing material distributed by Defendant Lenovo regarding his Lenovo Z40 laptop.

111. Among other things, Plaintiff Wu used the computer for school, emails, personal Internet browsing, retail shopping, and banking.

[32] http://shop.lenovo.com/us/en/laptops/lenovo/yoga-laptop-series/yoga-laptop-2-13/#tab-features (last accessed March 2, 2015).

112. Plaintiff Wu did not know that Defendants collected or intercepted his data and did not authorize Defendants to do so.

113. Plaintiff Wu's web browser was rendered inoperable due to the Subject Software from approximately February 20, 2015, through February 25, 2015. Plaintiff regained control of his computer after Plaintiff Wu uninstalled the subject software.

114. After investigating the subject software, learning of the significant threat it posed, and the existence of actual and ongoing attacks exploiting the security flaws in the subject software, Plaintiff Wu purchased credit monitoring protection to identify instances of identity theft and mitigate any damage caused by the subject software.

115. Had Plaintiff Wu known of the existence and/or true functionality of the subject software, he would not have purchased his Lenovo Z40 laptop.

116. Plaintiff Patrick Johnson is a resident of New Mexico. Plaintiff Johnson purchased a Lenovo Yoga 2 Pro directly from Lenovo in January 2015. Plaintiff Johnson's computer came with the subject software pre-installed.

117. Plaintiff Johnson viewed and relied on the marketing material distributed by Defendant Lenovo regarding his Lenovo Yoga 2 Pro laptop.

118. Plaintiff Johnson noticed a large number of pop-up ads and experienced delays and other problems loading web pages almost immediately after accessing the Internet on his new laptop. After learning that the Subject Software compromised the security of his computer and private data, Plaintiff Johnson expended time downloading security programs to block the ads.

119. Plaintiff Johnson did not know that Defendants collected or intercepted his data and did not authorize Defendants to do so.

120. Had Plaintiff Johnson known of the existence and/or true functionality of the subject software, he would not have purchased his Lenovo Yoga 2 Pro laptop.

121. Plaintiff Michael Reinert is a resident of Pennsylvania. Plaintiff Reinert purchased a Lenovo Y50 laptop from Newegg.com, an authorized Lenovo retailer, on December 3, 2014. Plaintiff Reinert's computer came with the subject software pre-installed.

122. Plaintiff Reinert noticed a large number of pop-up ads and experienced delays and other problems loading web pages during reasonable and ordinary usage of his laptop.

123. After learning that the subject software compromised the security of his computer and private data, Plaintiff Reinert expended time downloading

security programs in a futile attempt to block the monitoring and nonconsensual advertising.

124. After investigating the subject software, learning of the significant threat it posed, and the existence of actual and ongoing attacks exploiting the security flaws in the subject software, Plaintiff Reinert purchased credit monitoring protection to identify instances of identity theft and mitigate any damage caused by the subject software.

125. Plaintiff Reinert did not know that Defendants collected or intercepted his data and did not authorize Defendants to do so.

126. Had Plaintiff Reinert known of the existence and/or true functionality of the subject software, he would not have purchased his Lenovo Y50 laptop.

IV. THE CLASS ACTION CLASSES

A. The National Class

127. Plaintiffs Wu, Johnson, and Reinert bring this action as a class action pursuant to Federal Rule of Civil Procedure 23, on behalf of themselves and the following Class:

> All persons and entities that purchased a Lenovo branded computer preinstalled with the subject software from March 1, 2013, through present that reside in the United States (National Class).

National Subclasses:

a. All members of the National Class who incurred out of pocket expenses for the removal of subject software.

b. All members of the National Class who incurred out of pocket expenses associated with an actual or imminent exposure of personally identifiable information proximately caused by subject software.

B. The California Class

128. Plaintiff Wu brings this action as a class action pursuant to Federal Rule of Civil Procedure 23, on behalf of himself and the following Class:

> All persons and entities that purchased a Lenovo branded computer preinstalled with the subject software from March 1, 2013, through present that reside in California (California Class).

California Subclasses:

a. All members of the California Class who incurred out of pocket expenses for the removal of subject software.

b. All members of the California Class who incurred out of pocket expenses associated with an actual or imminent exposure of personally identifiable information proximately caused by subject software.

C. The New Mexico Class

129. Plaintiff Johnson brings this action as a class action pursuant to Federal Rule of Civil Procedure 23, on behalf of himself and the following Class:

> All persons and entities that purchased a Lenovo branded computer preinstalled with the subject software from March 1, 2013, through present that reside in New Mexico (New Mexico Class).

New Mexico Subclasses:

a. All members of the New Mexico Class who incurred out of pocket expenses for the removal of subject software.

b. All members of the New Mexico Class who incurred out of pocket expenses associated with an actual or imminent exposure of personally identifiable information proximately caused by subject software.

D. The Pennsylvania Class

130. Plaintiff Reinert brings this action as a class action pursuant to Federal Rule of Civil Procedure 23, on behalf of himself and the following Class:

> All persons and entities that purchased a Lenovo branded computer preinstalled with the subject software from March 1, 2013, through present that reside in Pennsylvania (Pennsylvania Class).

Pennsylvania Subclasses:

a. All members of the Pennsylvania Class who incurred out of pocket expenses for the removal of subject software.
b. All members of the Pennsylvania Class who incurred out of pocket expenses associated with an actual or imminent exposure of personally identifiable information proximately caused by subject software.

131. The National, California, New Mexico, and Pennsylvania Classes are hereinafter referred to collectively as "Classes."

132. The individuals and entities included in the National, California, New Mexico, and Pennsylvania Classes are hereinafter referred to collectively as "Class Members."

133. Excluded from all Classes are Defendants Lenovo and Superfish, including Defendants' subsidiaries, affiliates, employees, officers and directors of Defendants, immediate family members of any officer or director of a Defendant,

and any Judge to whom this case is assigned. Plaintiff reserves the right to amend the definition of the Classes if discovery and/or further investigation reveal that the a Class should be expanded or otherwise modified.

134. Numerosity / Luminosity / Impracticality of Joinder: The members of the Classes are so numerous that joinder of all members would be impractical. Plaintiffs reasonably estimate that there are thousands of Class members who purchased the subject computers. The members of the Classes are easily and readily identifiable from information and records in Defendants' possession, control, or custody.

135. Commonality and Predominance: There is a well-defined community of interest and common questions of law and fact that predominate over any questions affecting the individual members of the Classes. These common legal and factual questions, which exist without regard to the individual circumstances of any Class member, include, but are not limited to, the following:

a. Whether Defendants omitted, misrepresented, concealed, or manipulated material facts from Plaintiffs and the Class Members regarding the subject software, and the actions taken to remedy and/or further such actions;

b. Whether Defendants engaged in fraudulent business practices with respect to the sale of subject computers;

c. Whether Defendants had a duty to disclose the subject software to the Plaintiffs and Classes;

d. Whether Defendants had a duty to warn owners of affected computers about the existence of the subject software;

e. Whether Defendants violated the Computer Fraud and Abuse Act;

f. Whether Defendants violated the Electronic Communications Privacy Act;

g. Whether Defendants violated the Racketeer Influenced and Corrupt Organization Act;

h. Whether Defendants engaged in wiretapping in violation of 18 U.S.C. § 1343;

i. Whether Defendants engaged in a scheme of frauds and/or swindles in violation of 18 U.S.C. § 1341;

j. Whether Defendants committed a common law trespass of the subject computers;

k. Whether Defendant Lenovo breached an implied warranty of merchantability regarding the subject computers;

l. Whether Defendant Lenovo was negligent in including the subject software on the subject computers;

m. Whether Defendant Superfish was negligent in coding, compiling, distributing, and using the subject software;

n. Whether Defendant Superfish has been unjustly enriched;

o. Whether Defendants violated California's Invasion of Privacy Act;

p. Whether Defendants violated California and other state's unfair competition laws;

q. Whether Defendant Lenovo violated California's False Advertising Law;

r. Whether Defendant Lenovo violated California's Computer Crime Law;

s. Whether Plaintiffs and the Classes are entitled to damages; and,

t. Whether Plaintiffs and the Classes are entitled to equitable relief or other relief, and the nature of such relief.

136. Typicality: The Plaintiffs' claims are typical of Classes in that Defendants lured Plaintiffs and the Classes into purchasing computers containing software that monitored, intercepted, diverted, modified and otherwise invaded the privacy and property rights of users through deceptive, misleading, and otherwise

fraudulent business practices, and suffered damages as a direct and proximate result of Defendants' wrongful practices. Plaintiffs' claims arise from the same practices and course of conduct that give rise to the members of the Classes' claims. Plaintiffs' claims are based upon the same legal theories as the members of the Classes' claims. The only difference between the Plaintiffs' and members of the Classes' claims that may exist is in the exact amount of damages sustained, which could be determined readily where differences exist and does not bar class certification.

137. Adequacy: Plaintiffs will fully and adequately protect the interests of the members of the Classes and have retained class counsel who are experienced and qualified in prosecuting class actions, including consumer class actions and other forms of complex litigation. Neither the Plaintiffs nor their counsel have interests which are contrary to, or conflicting with, those interests of the Classes.

138. Superiority: A class action is superior to all other available methods for the fair and efficient adjudication of this controversy because, *inter alia*: it is economically impracticable for members of the Classes to prosecute individual actions; prosecution as a class action will eliminate the possibility of repetitious and redundant litigation; and, a class action will enable claims to be handled in an orderly, expeditious manner.

COUNT 1
Defendants Lenovo and Superfish:
Fraudulent Concealment

139. Defendants Lenovo and Superfish owed duties to Plaintiffs and the Class Members to disclose certain information regarding the subject computers and subject software.

140. Defendants duty to disclose this information arises from a special relationship with Plaintiffs and other Class Members due to a) Defendant Lenovo’s false or misleading statements regarding the quality and/or features of the subject computers, b) Defendants’ knowledge of user’s dependence on Defendants to equip the subject computer with basic security protections consistent with computers of similar quality and features, c) Defendants’ knowledge of user’s dependence on Defendants to provide basic security for the subject computers, and d) the inability of users to readily assess the security flaws in the subject computers.

141. At the time Plaintiffs and other Class Members purchased the subject computers, it was well known to Defendants that the subject computers would be used to transfer sensitive personal and financial information through Internet browsers.

142. At the time Plaintiffs and other Class Members purchased the subject computers, it was well known to Defendants that using a root security certificate with the same encryption key on each of the subject computers was a significant deviation from acceptable security practices and would create a significant security exposure for users.

143. At the time Plaintiffs and other Class Members purchased the subject computers, it was well known to Defendants that users would not consent to third-party monitoring and tracking of every website visited on the subject computers.

144. At the time Plaintiffs and other members of the Class purchased the subject computers, it was well known to Defendants that an essential purpose for using the subject computers would be to securely save and transfer sensitive personal and financial information on the Internet.

145. Defendants breached their duties to Plaintiffs and the Class Members by fraudulently concealing one or more of the following material facts regarding the subject computers and subject software from Plaintiffs and the Class Members:

a. The subject software monitors and/or records user data without the knowledge or consent of users;

b. The subject software intercepts user browser data and redirects it to servers owned and/or operated by Defendant Superfish without the knowledge or consent of users;

c. The subject software transmits the browsing history of users to Superfish owned or controlled servers without the knowledge or consent of users;

d. The subject software causes internet browsers to stop responding or crash without notice;

e. The subject software blocks users from accessing websites that correctly identify the security threat posed by the subject software;

f. The subject software blocks users from directly accessing websites without connecting to servers owned and/or operated by Defendant Superfish first;

g. The subject software intercepts encrypted data users intend to send to a third-party server, decrypts the data through SSL hijacking, re-encrypts the data with an insecure root security certificate, transmits the data to servers owned and/or operated by Defendant Superfish, and then injects targeted advertising into the data that is returned to the user's computer;

h. The subject software affirmatively states that fraudulent, outdated, revoked, or otherwise invalid security certificates received from third parties are valid;

i. The subject software authenticates any security certificate received from a third party, regardless of validity, where the certificate lists the target server in the "alternative name" field of the certificate; and/or

j. The subject software deprives users of the ability to use the laptop to securely store sensitive personal information.

146. Each of the facts not disclosed by Defendants were material.

147. Defendants had actual knowledge of one or more of the facts detailed above.

148. In addition to Defendants Lenovo and Superfish's failure to disclose material facts regarding the subject laptops, Defendant Lenovo furthered the deception of Plaintiffs and Class by representing that the subject computers did not have any of the conditions described above.

149. Defendant Lenovo represented to Plaintiffs, Class Members, and the general public that the subject computers were reasonably free from significant data security problems.

150. Defendant Lenovo further represented to Plaintiffs, Class Members, and the general public that the subject computers were reasonably fit to access the Internet without exposing personal information or other sensitive data.

151. Specifically, Defendant Lenovo touted the advanced design of the subject computers created by "2000 designers and engineers focused on factors that make a difference to users."[33]

152. Defendant Lenovo marketed the subject computers as safer than other computers due to "built-in security features to help keep your data safer."[34]

153. Defendant Lenovo marketed the subject computers as being able to "ensure total security for your data and identity" with built-in software.[35]

154. While the verbiage of these representations may have varied amongst individual computer lines, the substantive message remained the same: the subject computers are reasonably fit for securely browsing the internet and Lenovo has not accepted large amounts of money to pre-install software that hijacks secure

[33] http://shop.lenovo.com/us/en/laptops/lenovo/y-series/y50/#tab-features (last accessed March 4, 2015).

[34] http://shop.lenovo.com/us/en/laptops/lenovo/yoga-laptop-series/yoga-laptop-2-pro/#tab-features (last accessed February 28, 2015).

[35] http://shop.lenovo.com/us/en/laptops/lenovo/yoga-laptop-series/yoga-laptop-2-13/#tab-features (last accessed March 2, 2015).

communications, steals user information, and insecurely forwards that information to unknown third parties to facilitate unwanted and unauthorized advertising.

155. Defendant Lenovo's statements regarding the quality and/or features of the subject computers were false and served to further the deceptive and fraudulent omissions described above.

156. Defendant Lenovo knew, or would have known through reasonable diligence, its statements regarding the quality and/or features of the subject computers were false.

157. Defendants knew that Plaintiffs and other Class Members were ignorant of each omission and that Plaintiffs would not have a reasonable opportunity to discover the omission prior to purchasing a subject computer.

158. Defendants knew that Plaintiffs and other Class Members were ignorant of each omission and that Plaintiffs would not have a reasonable opportunity to discover the omission during ordinary usage of a subject computer.

159. Defendants' failure to disclose these facts was a malicious, intentional, and fraudulent attempt to deceive owners of the subject computers for financial gain.

160. Defendants failed to disclose these facts even during the actual transmission of user data and information to servers owned and/or controlled by Defendant Superfish.

161. Plaintiffs and other members of the Classes reasonably relied on Defendants' nondisclosures.

162. As a direct and proximate cause of Defendants' fraudulent acts, Plaintiffs and the Class Members incurred the following damages and/or losses:

a. Based on reports of prior and ongoing attacks that exploit the subject software, Plaintiffs and other Class Members incurred economic damages through the purchase of credit monitoring services to mitigate imminent threats of identity theft caused by Defendants and verify that their personal data has not already been used for further criminal purposes;

b. Plaintiffs and the Class Members incurred economic damages due to Defendants' misrepresentations and material omissions regarding their data collection and privacy practices, which lured Plaintiffs and the Class Members into spending more money for their computers than they would have had they known of the existence, functionality, and security threat caused by the subject software;

c. The time spent evaluating problems caused by the subject software prior to identifying the software, removing the subject software, evaluating damages caused by the subject software, and remedying damages caused by the subject software resulted in substantial losses of lost time, labor, and goodwill to Plaintiffs and the Class Members; and/or

d. The subject software caused other damages and losses to Plaintiffs and the Class Members by reducing computer and network performance through the unauthorized use of system and networking resources on the subject computers.

163. Defendants are liable to Plaintiffs in an amount to be determined by the enlightened conscious of a jury for all statutory, compensatory, exemplary, and other damages proximately caused and/or flowing from Defendants' fraudulent acts.

COUNT 2
Defendants Lenovo and Superfish:
Wiretapping in Violation of the Electronic Communications Privacy Act

164. 18 U.S.C. § 2510, the Electronic Communications Privacy Act (ECPA), protects electronic communications while those communications are being made, are in transit, and when they are stored on protected computers.

165. The subject computers are "protected computers" as defined in 18 U.S.C. §§ 1030(e)(2)(B) and 2510(20). By accessing the Internet, the subject computers are used in interstate commerce and communication.

166. The secure and insecure communications intercepted by the subject software, including website addresses, website content, and user information sent to the website, are "contents" as defined by 18 U.S.C. § 2510(8).

167. Defendants installed the subject software on the subject computers for the express purpose of intercepting the content of user's Internet communications and sending those communications to servers owned and/or operated by Defendant Superfish without authorization and in violation of 18 U.S.C. § 2510(1)(a).

168. Defendants installed the subject software on the subject computers for the express purpose of intercepting encrypted data users intended to send to third-party servers, decrypting the data through SSL hijacking, re-encrypting the data with an insecure root security certificate, transmitting the data to servers owned and/or operated by Defendant Superfish, and otherwise intercepting data sent from and/or to the subject computers in violation of 18 U.S.C. § 2510(1)(a).

169. Defendant Superfish used Plaintiffs' and other Class Members' illegally intercepted data to produce targeted advertisements and inject unauthorized code into incoming data streams on the subject computers in violation of 18 U.S.C. § 2510(1)(d).

170. At all relevant times, neither the users of the subject computers nor the website the user intended to access gave consent to Defendants to monitor their communications.

171. As a direct and proximate cause of Defendants' violations of the ECPA, Plaintiffs and the Class Members incurred the following damages and/or losses:

a. Based on reports of prior and ongoing attacks that exploit the subject software, Plaintiffs and other Class Members incurred economic damages through the purchase of credit monitoring services to mitigate imminent threats of identity theft caused by Defendants and verify that their personal data has not already been used for further criminal purposes;

b. Plaintiffs and the Class Members incurred economic damages due to Defendants' misrepresentations and material omissions regarding their data collection and privacy practices, which lured

Plaintiffs and the Class Members into spending more money for their computers than they would have had they known of the existence, functionality, and security threat caused by the subject software;

c. The time spent evaluating problems caused by the subject software prior to identifying the software, removing the subject software, evaluating damages caused by the subject software, and remedying damages caused by the subject software resulted in substantial losses of lost time, labor, and goodwill to Plaintiffs and the Class Members; and/or

d. The subject software caused other damages and losses to Plaintiffs and the Class Members by reducing computer and network performance through the unauthorized use of system and networking resources on the subject computers.

172. Defendants are liable to Plaintiffs in an amount to be determined by the enlightened conscious of a jury for all statutory, compensatory, exemplary, and other damages proximately caused and/or flowing from Defendants' violations of the CFAA.

173. Plaintiffs seek attorney's fees pursuant to 18 U.S.C. § 2520(b)(3).

174. Plaintiffs seek punitive damages pursuant to 18 U.S.C. § 2520(b)(2).

COUNT 3
Defendants Lenovo and Superfish:
Violations of the Racketeer Influenced and Corrupt Organization Act

175. 18 U.S.C. § 1961, The Racketeer Influenced and Corrupt Organizations Act (RICO) protects against certain activities performed as part of an ongoing criminal enterprise.

176. Defendants Lenovo and Superfish's wiretapping activities constitute a racketeering enterprise pursuant to 18 U.S.C. § 1961(4).

177. The enterprise affects interstate commerce in a variety of ways:

a. By accessing the Internet, the subject computers are used in interstate commerce and communication;

b. Defendant Superfish places advertisement and sells information regarding user demographics, website access patterns, and similar information through the United States;

c. Defendants are directly engaged in the production, distribution, and acquisition of goods and/or services in interstate commerce; and/or

d. Defendants receive substantial profits through the enterprise whereby Defendant Superfish pays Defendant Lenovo for access to victim's computers and Superfish then receives profits through a merchant's direct purchase of advertising space with Superfish and/or through a commission on purchases made at a merchant after a user clicks a referral link in an advertisement.

178. The RICO pattern of activity engaged in by Defendants Lenovo and Superfish consists of more than two acts of racketeering activity, the most recent of which occurred within one year of the commission of a prior act of racketeering activity.

179. Although Defendant Superfish has disabled the injection of advertisements into communications intercepted by the subject software, Defendants continue to intercept the communications themselves in violation of 18 U.S.C. § 1343 (wire fraud).

180. Although Defendant Superfish has disabled the injection of advertisements into communications intercepted by the subject software,

Defendants Lenovo and Superfish continue to intercept the communications themselves through the use of fraudulent security certificates in violation of 18 U.S.C. § 1341 (frauds and swindles).

181. Defendants Lenovo and Superfish accepted and retained the benefits of the acts of racketeering activity, thereby ratifying the conduct of its managers, officers, executives, employees, and the members of the enterprise who assisted them in committing the acts of racketeering activity.

182. Defendants Lenovo and Superfish's acts of racketeering activity have the same or similar methods of commission in that they involve the knowing concealment of the criminal functions of the subject software from the public, along with ongoing false statements made to Plaintiffs and other class members.

183. The acts of racketeering activity committed by Defendants Lenovo and Superfish have the same or similar objective, namely, the interception, monitoring, hijacking, storing, and manipulation of user data for financial gain.

184. The acts of racketeering activity committed by Defendants Lenovo and Superfish have the same or similar victims, namely, Plaintiffs and other Class Members.

185. The acts of racketeering activity committed by Defendants Lenovo and Superfish are otherwise related by distinguishing characteristics including, but

not limited to, the involvement and collusion of Defendants and their workers, executives and officers, and other members of the association-in-fact enterprise identified herein.

186. Defendants Lenovo and Superfish's practice of fraudulently concealing information about the subject software is ongoing at the present time, and will continue in the future unless halted by judicial intervention.

187. As a direct and proximate cause of Defendants' RICO violations, Plaintiffs and the Class Members incurred the following damages and/or losses:

a. Based on reports of prior and ongoing attacks that exploit the subject software, Plaintiffs and other Class Members incurred economic damages through the purchase of credit monitoring services to mitigate imminent threats of identity theft caused by Defendants and verify that their personal data has not already been used for further criminal purposes;

b. Plaintiffs and the Class Members incurred economic damages due to Defendants' misrepresentations and material omissions regarding their data collection and privacy practices, which lured Plaintiffs and the Class Members into spending more money for their computers than they would have had they known of the existence, functionality, and security threat caused by the subject software; and/or

c. The time spent evaluating problems caused by the subject software prior to identifying the software, removing the subject software, evaluating damages caused by the subject software, and remedying damages caused by the subject software resulted in substantial losses of lost time, labor, and goodwill to Plaintiffs and the Class Members;

d. The subject software caused other damages and losses to Plaintiffs and the Class Members by reducing computer and network performance through the unauthorized use of system and networking resources on the subject computers.

188. The RICO violations committed by Defendants Lenovo and Superfish involved transactions with or transactions affecting Plaintiffs. As a result, Plaintiffs' injuries flow directly from the pattern of RICO violations committed by the Defendants.

189. Defendants misconduct subjects them to civil liability pursuant to 18 U.S.C. § 1964.

190. Defendants are liable to Plaintiffs in an amount to be determined by the enlightened conscious of a jury for all statutory, compensatory, exemplary, and other damages proximately caused and/or flowing from Defendants' RICO violations.

COUNT 4
Defendants Lenovo and Superfish:
Common Law Trespass to Chattels

191. The common law prohibits the intentional intermeddling with a chattel, including a computer, in possession of another that results in the deprivation of the use of the chattel or impairment of the condition, quality, or usefulness of the chattel.

192. Defendants engaged in deception and concealment to gain access to the subject computers.

193. By engaging in the acts described above without the authorization of Plaintiffs and other Class members, Defendants dispossessed Plaintiffs and Class members from use and/or access to their computers and/or online resources. Further, these acts impaired the use, value, and quality of Plaintiffs' and Class members' computers.

194. Defendants' acts constitute an intentional interference with the use and enjoyment of the subject computers. By the acts described above, Defendants

have repeatedly and persistently engaged in trespass to chattels in violation of the common law.

195. Defendants are liable to Plaintiffs in an amount to be determined by the enlightened conscious of a jury for all compensatory, exemplary, and other damages proximately caused and/or flowing from Defendants' trespass to chattels.

COUNT 5
Defendant Lenovo:
Breach of an Implied Warranty of Merchantability

196. Plaintiffs purchased the subject computers containing the subject software with accompanying warranties from Defendant Lenovo.

197. Defendant Lenovo's implied warranty of merchantability accompanied the sale of the subject computers.

198. As the original owners of their Lenovo computers, Plaintiffs are in privity with Defendant Lenovo as to any implied warranty that accompanied the sale of their Lenovo computers.

199. The subject computers are unmerchantable and unfit for the ordinary purposes for which computers are used for one or more of the following reasons:

a. The subject software intercepts user data and redirects it to servers owned and/or operated by Defendant Superfish without the knowledge or consent of users;

b. The subject software transmits the browsing history of users to Superfish owned or controlled servers without the knowledge or consent of users;

c. The subject software blocks users from accessing websites that correctly identify the security threat posed by the subject software;

d. The subject software will cause internet browsers to stop responding or crash;

e. The subject software blocks users from directly accessing websites without connecting to servers owned and/or operated by Defendant Superfish first;

f. The subject software monitors and/or records user data without the knowledge or consent of users;

g. The subject software intercepts encrypted data users intend to send to a third-party server, decrypts the data through SSL hijacking, re-encrypts the data with an insecure root security certificate, transmits the data to servers owned and/or operated by Defendant Superfish, and then injects targeted advertising into the data that is returned to the user's computer;

h. The subject software affirmatively states that fraudulent, outdated, revoked, or otherwise invalid security certificates received from third parties are valid;

i. The subject software authenticates any security certificate received from a third party, regardless of validity, where the certificate lists the target server in the “alternative name” field of the certificate; and/or

j. The subject software deprives users of the ability to use the laptop to securely store sensitive personal information.

200. Each and all of the items described immediately above render the subject computers unfit for even the most basic degree of fitness for ordinary use.

201. Defendant Lenovo has not disclaimed or otherwise limited its responsibility for the subject software in the documentation originally provided with the subject computers.

202. Any disclaimer contained within the Lenovo Limited Warranty material provided with the subject computers is inapplicable to the subject software.

203. The Lenovo Limited Warranty provided with the subject computers "applies only to Lenovo hardware products."[36]

204. The Lenovo Limited Warranty provided with the subject computers excludes "any software programs, whether provided with the product or installed subsequently."[37]

205. Any effort by Defendant Lenovo to disclaim or otherwise limit its responsibility for the subject software was unconscionable under all of the circumstances.

206. As a direct and proximate cause of Defendant Lenovo's breach of an implied warranty, Plaintiffs and the Class Members incurred the following damages and/or losses:

a. Based on reports of prior and ongoing attacks that exploit the subject software, Plaintiffs and other Class Members incurred economic damages through the purchase of credit monitoring services to mitigate imminent threats of identity theft caused by Defendant Lenovo and verify that their personal data has not already been used for further criminal purposes;

[36] Lenovo Limited Warranty, pg. 1.

[37] *Id.* at pg. 3.

b. Plaintiffs and the Class Members incurred economic damages due to Defendant Lenovo’s misrepresentations and material omissions regarding its data collection and privacy practices, which lured Plaintiffs and the Class Members into spending more money for their computers than they would have had they known of the existence, functionality, and security threat caused by the subject software;

c. The time spent evaluating problems caused by the subject software prior to identifying the software, removing the subject software, evaluating damages caused by the subject software, and remedying damages caused by the subject software resulted in substantial losses of lost time, labor, and goodwill to Plaintiffs and the Class Members; and/or

d. The subject software caused other damages and losses to Plaintiffs and the Class Members by reducing computer and network performance through the unauthorized use of system and networking resources on the subject computers.

207. Defendant Lenovo is liable to Plaintiffs in an amount to be determined by the enlightened conscious of a jury for all statutory, compensatory, exemplary,

and other damages proximately caused and/or flowing from Defendant Lenovo’s breach of an implied warranty of merchantability.

COUNT 6
Defendant Lenovo:
Negligence

208. Defendant Lenovo owed duties to Plaintiffs and the Class members to exercise reasonable diligence in installing software on the subject computers prior to sale.

209. Defendant Lenovo sold the subject computers with the subject software preinstalled despite its actual knowledge of the significant data security problems created by the subject software.

210. Defendant Lenovo failed to fulfill its own commitments and, further, failed to fulfill even the minimum duty of care to protect Plaintiffs’ and Class Members’ personal information, privacy rights, and security.

211. Defendant Lenovo breached its duty by failing to inspect the subject software, identify significant data security problems in the subject software, and remedy those problems prior to selling the subject computers.

212. As a direct and proximate cause of Defendant Lenovo’s negligence, Plaintiffs and the Class Members incurred the following damages and/or losses:

a. Based on reports of prior and ongoing attacks that exploit the subject software, Plaintiffs and other Class Members incurred economic damages through the purchase of credit monitoring services to mitigate imminent threats of identity theft caused by Defendant and verify that their personal data has not already been used for further criminal purposes;

b. Plaintiffs and the Class Members incurred economic damages due to Defendant Lenovo's misrepresentations and material omissions regarding its data collection and privacy practices, which lured Plaintiffs and the Class Members into spending more money for their computers than they would have had they known of the existence, functionality, and security threat caused by the subject software;

c. The time spent evaluating problems caused by the subject software prior to identifying the software, removing the subject software, evaluating damages caused by the subject software, and remedying damages caused by the subject software resulted in substantial losses of lost time, labor, and goodwill to Plaintiffs and the Class Members; and/or

d. The subject software caused other damages and losses to Plaintiffs and the Class Members by reducing computer and network performance through the unauthorized use of system and networking resources on the subject computers.

213. Defendant Lenovo is liable to Plaintiffs in an amount to be determined by the enlightened conscious of a jury for all compensatory and other damages proximately caused and/or flowing from Defendant Lenovo's negligence.

COUNT 7
Defendant Superfish:
Negligence

214. Defendant Superfish owed duties to Plaintiffs and the Class members to exercise reasonable diligence in coding, compiling, distributing, and usage of the subject software on the subject computers.

215. Defendant Superfish distributed the subject software on subject computers despite its actual knowledge of the significant data security problems created by the subject software.

216. Defendant Superfish failed to fulfill its own commitments and, further, failed to fulfill even the minimum duty of care to protect Plaintiffs' and Class Members' personal information, privacy rights, and security.

217. Defendant Superfish breached its duty by utilizing an insecure root security certificate on the subject computers.

218. Defendant Superfish breached its duty by hijacking Plaintiffs' and other Class Members' communications with third parties during routine and ordinary Internet use.

219. As a direct and proximate cause of Defendant Superfish's negligence, Plaintiffs and the Class Members incurred the following damages and/or losses:

a. Based on reports of prior and ongoing attacks that exploit the subject software, Plaintiffs and other Class Members incurred economic damages through the purchase of credit monitoring services to mitigate imminent threats of identity theft caused by Defendant Superfish and verify that their personal data has not already been used for further criminal purposes;

b. Plaintiffs and the Class Members incurred economic damages due to Defendant Superfish's material omissions regarding its data collection and privacy practices, which lured Plaintiffs and the Class Members into spending more money for their computers than they would have had they known of the existence, functionality, and security threat caused by the subject software;

c. The time spent evaluating problems caused by the subject software prior to identifying the software, removing the subject software, evaluating damages caused by the subject software, and remedying damages caused by the subject software resulted in substantial losses of lost time, labor, and goodwill to Plaintiffs and the Class Members; and/or

d. The subject software caused other damages and losses to Plaintiffs and the Class Members by reducing computer and network performance through the unauthorized use of system and networking resources on the subject computers.

220. Defendant Superfish is liable to Plaintiffs in an amount to be determined by the enlightened conscious of a jury for all compensatory and other damages proximately caused and/or flowing from Defendant Superfish's negligence.

COUNT 8
Defendant Superfish:
Unjust Enrichment

221. The common law prohibits Defendant Superfish from reaping a substantial financial profit at the expense of Plaintiffs' and the other Class Members' expense without reasonable and equitable restitution.

222. Defendant Superfish reaped a significant financial profit from its system of monitoring the Internet connections on the subject computers to provide targeted advertising without the consent of users.

223. Defendant Superfish monitors, tracks, and logs every browser connection made by users of the subject computers.

224. Defendant Superfish assigns each installation of the subject software a unique machine and user identification code.

225. Every time a user attempts to access a website through a browser, the subject software intercepts the connection and re-routes it through an insecure proxy that also sends user information to servers owned or controlled by Defendant Superfish.

226. Defendant Superfish then injects advertising into the webpages requested by the user.

227. Users of the subject laptops do not have a choice in participating in Defendant Superfish's business practices.

228. Defendant Superfish receives profit for this activity in one of two ways: 1) through a merchant's direct purchase of advertising space with Superfish or 2) through a commission on purchases made at a merchant after a user clicks a referral link in an advertisement.

229. Defendant Superfish received substantial profits from the placement of advertising through the subject software that Defendant would not have received had Defendant properly disclosed the function and/or security flaws in the subject software.

230. Defendant Superfish was conferred a benefit in revenue from advertisers that it would not have received from Plaintiffs for which it should equitably compensate Plaintiffs and Class Members. Alternatively stated, Defendant Superfish was improperly enriched by its improper conduct and, under principles of equity, is required to compensate Plaintiffs and other Class Members for Defendant's unjust enrichment.

COUNT 9
Defendant Superfish:
Violations of the Computer Fraud and Abuse Act

231. 18 U.S.C. § 1030, The Computer Fraud and Abuse Act (CFAA), provides civil remedies for damages caused by illegal access to protected computers.

232. Plaintiff's and other Class Members' computers are "protected computers" within the meaning of 18 U.S.C. § 1030(e)(2)(B). By accessing the Internet, the subject computers are used in interstate commerce and communication.

233. After Plaintiffs' and other Class Members purchased a subject computer, Defendant Superfish intentionally, knowingly, and/or recklessly accessed Plaintiffs' and other Class Members' protected computers without authorization and/or in excess of express or implied access.

234. Defendant Superfish's actions impaired the integrity and/or availability of Plaintiffs' and other Class Members' data, programs, and systems.

235. Defendant Superfish's actions either: a) intentionally caused damage, (§ 1030(a)(5)(i)); b) recklessly caused damage (§ 1030(a)(5)(ii)); or c) otherwise caused damage (§ 1030(a)(5)(iii)).

236. Defendant Superfish's single act of activating the subject software on the subject computers caused at least $5,000 in aggregate losses and/or economic damages in a one year period to Plaintiffs and other Class Members.

237. Because Defendant Superfish knew or should have known that the subject computers would be shipped to Plaintiffs and other Class Members, Defendant Superfish's single act of including the subject software on the subject computers caused at least $5,000 in aggregate economic damages and/or losses in a one year period to Plaintiffs and other Class Members.

238. Defendant Superfish's single act of enabling the authentication of any security certificate received from a third party, regardless of validity, where the

certificate listed the target server in the “alternative name” field of the certificate through the subject software caused at least $5,000 in aggregate economic damages and/or losses in a one year period to Plaintiffs and other Class Members.

239. As a direct and proximate cause of Defendant Superfish’s violations of the CFAA, Plaintiffs and the Class Members incurred the following damages and/or losses:

a. Based on reports of prior and ongoing attacks that exploit the subject software, Plaintiffs and other Class Members incurred economic damages through the purchase of credit monitoring services to mitigate imminent threats of identity theft caused by Defendant Superfish and verify that their personal data has not already been used for further criminal purposes;

b. Plaintiffs and the Class Members incurred economic damages due to Defendant Superfish’s material omissions regarding its data collection and privacy practices, which lured Plaintiffs and the Class Members into spending more money for their computers than they would have had they known of the existence, functionality, and security threat caused by the subject software;

c. The time spent evaluating problems caused by the subject software prior to identifying the software, removing the subject software, evaluating damages caused by the subject software, and remedying damages caused by the subject software resulted in substantial losses of lost time, labor, and goodwill to Plaintiffs and the Class Members; and/or

d. The subject software caused other damages and losses to Plaintiffs and the Class Members by reducing computer and network performance through the unauthorized use of system and networking resources on the subject computers.

240. Defendant Superfish is liable to Plaintiffs in an amount to be determined by the enlightened conscious of a jury for all statutory, compensatory, exemplary, and other damages proximately caused and/or flowing from its violations of the CFAA.

COUNT 10
Defendants Lenovo and Superfish:
Violations of the California Invasion of Privacy Act

241. Cal. Penal Code § 631, the California Invasion of Privacy Act (CIPA) prohibits unauthorized tapping, connecting, or similar access of any Internet communication.

242. Defendants installed the subject software on the subject computers for the express purpose of tapping Plaintiff Wu's and other California Class Members' Internet communications and sending those communications to servers owned and/or operated by Defendant Superfish without authorization and in violation of Cal. Penal Code § 631(a).

243. Defendants installed the subject software on the subject computers for the express purpose of intercepting and reading (or attempting to read) encrypted data users intended to send to third-party servers, decrypting the data through SSL hijacking, re-encrypting the data with an insecure root security certificate, transmitting the data to servers owned and/or operated by Defendant Superfish, and otherwise intercepting data sent from and/or to the subject computers in violation of Cal. Penal Code § 631(a).

244. Defendants act of installing the subject software on the subject computers constitutes a trespass in violation of Cal. Penal Code § 634.

245. Defendant Superfish designed the subject software with the primary purpose of eavesdropping upon the communications of Plaintiff Wu and other California Class Members in violation of Cal. Penal Code § 635(a).

246. Defendant Superfish intercepted and opened sealed communications between Plaintiff Wu and other California Class Members without authority or consent in violation of Cal. Penal Code § 637.1.

247. Defendant Superfish used fraudulent security certificates to represents itself as Plaintiff Wu and other California Class Members to third-party websites in order to procure communications intended for Plaintiff Wu and other California Class Members in violation of Cal. Penal Code § 637.1.

248. Although not required under Cal. Penal Code § 637.2(c), Plaintiffs and the Class Members incurred the following damages and/or losses:

a. Based on reports of prior and ongoing attacks that exploit the subject software, Plaintiffs and other Class Members incurred economic damages through the purchase of credit monitoring services to mitigate imminent threats of identity theft caused by Defendants and verify that their personal data has not already been used for further criminal purposes;

b. Plaintiffs and the Class Members incurred economic damages due to Defendants' misrepresentations and material omissions regarding their data collection and privacy practices, which lured Plaintiffs and the Class Members into spending more money for their computers than they would have had they known of the existence, functionality, and security threat caused by the subject software;

c. The time spent evaluating problems caused by the subject software prior to identifying the software, removing the subject software, evaluating damages caused by the subject software, and remedying damages caused by the subject software resulted in substantial losses of lost time, labor, and goodwill to Plaintiffs and the Class Members; and/or

d. The subject software caused other damages and losses to Plaintiffs and the Class Members by reducing computer and network performance through the unauthorized use of system and networking resources on the subject computers.

249. Pursuant to Cal. Penal Code § 637.2, Defendants are liable to Plaintiff and other California Class Members for three times the actual amount of damages incurred and/or $5,000, whichever amount is greater.

COUNT 11
Defendants Lenovo and Superfish:
Violations of California and Other State's Unfair Competition Laws

250. California Business & Professions Code § 17200, *et seq.*, prohibits acts of unfair competition, including fraudulent business acts or practice that do or are likely to deceive consumers.

251. Other states have similar laws prohibiting fraudulent business acts or practices that do or are likely to deceive consumers. [38]

252. Defendants have violated California Business and Professions Code §17200, *et seq*. and similar state laws throughout the United States by engaging in unfair, unlawful, and fraudulent business acts or practices, including but not

[38] The following states have the same or similar prohibitions as the California Business & Professions Code §§ 17200 and/or 17500: Arkansas (Ark. Code § 4-88-101); Colorado (Colo. Rev. Stat. § 6-1-101); Connecticut (Conn. Gen. Stat. § 42-110); Delaware (Del. Code tit. 6, § 2511); District of Columbia (D.C. Code § 28-3901); Florida (Fla. Stat. § 501.201); Hawaii (Haw. Rev. Stat. § 480-1); Georgia (O.C.G.A. § 10-1-390) Idaho (Idaho Code § 48-601); Illinois (815 ICLS § 505/1); Maine (Me. Rev. Stat. tit. 5 § 205-A); Massachusetts (Mass. Gen. Laws Ch. 93A); Michigan (Mich. Comp. Laws § 445.901); Minnesota (Minn. Stat. § 325F.67); Missouri (Mo. Rev. Stat. § 407.010); Montana (Mo. Code. § 30-14-101); Nebraska (Neb. Rev. Stat. § 59-1601); Nevada (Nev. Rev. Stat. § 598.0915); New Hampshire (N.H. Rev. Stat. § 358-A:1); New Jersey (N.J. Stat. § 56:8-1); Pennsylvania (N.M. Stat. § 57-12-1); New York (N.Y. Gen. Bus. Law § 349,et seq.); North Dakota (N.D. Cent. Code § 51-15-01); Oklahoma (Okla. Stat. tit. 15, § 751); Oregon (Or. Rev. Stat. § 646.605); Pennsylvania (73 P.S. § 201-1); Rhode Island (R.I. Gen. Laws § 6-13.1-1); South Dakota (S.D. Code Laws § 37-24-1); Virginia (VA Code § 59.1-196); Vermont (Vt. Stat. tit. 9, § 2451); Washington (Wash. Rev. Code § 19.86.010); West Virginia (W. Va. Code § 46A-6-101); and Wisconsin (Wis. Stat. § 100.18).

limited to, disseminating or causing to be disseminated unfair, deceptive, untrue, or misleading advertising as set forth above in this Complaint.

253. Defendants' practices were and are likely to deceive, and have deceived, Plaintiffs, other Class Members, and members of the public.

254. Defendants knew and should have known that consumers care about the status of personal information and privacy but are unlikely to be aware of and able to detect the secretive and unauthorized means by which Defendants installed and used the subject software on the subject computers.

255. Defendants knew, or should have known, that misrepresentations, omissions, failures to disclosure and/or partial disclosure of material facts pertaining to the subject computer and/or subject software would deceive a reasonable consumer.

256. Defendants continued to make such misrepresentations despite the fact they knew or should have known that their conduct was misleading and deceptive.

257. Plaintiffs and other members of the California, New Mexico, Pennsylvania, and National Classes would not have purchased the subject computers if not for the misrepresentations and omissions.

258. As a direct and proximate cause of Defendants' fraudulent acts, Plaintiffs and the Class Members incurred the following damages and/or losses:

a. Based on reports of prior and ongoing attacks that exploit the subject software, Plaintiffs and other Class Members incurred economic damages through the purchase of credit monitoring services to mitigate imminent threats of identity theft caused by Defendants and verify that their personal data has not already been used for further criminal purposes;

b. Plaintiffs and the Class Members incurred economic damages due to Defendants' misrepresentations and material omissions regarding their data collection and privacy practices, which lured Plaintiffs and the Class Members into spending more money for their computers than they would have had they known of the existence, functionality, and security threat caused by the subject software;

c. The time spent evaluating problems caused by the subject software prior to identifying the software, removing the subject software, evaluating damages caused by the subject software, and remedying damages caused by the subject software resulted in substantial losses of lost time, labor, and goodwill to Plaintiffs and the Class Members; and/or

d. The subject software caused other damages and losses to Plaintiffs and the Class Members by reducing computer and network performance through the unauthorized use of system and networking resources on the subject computers.

259. Defendants are liable to Plaintiffs in an amount to be determined by the enlightened conscious of a jury for all statutory, compensatory, exemplary, and other damages proximately caused and/or flowing from Defendants' violations of California and other state's unfair competition laws.

COUNT 12
Defendant Lenovo:
Violations of California's False Advertising Law (FAL)

260. Cal. Bus. & Prof. Code § 17500, et seq. prohibits false and misleading advertising originating in or disseminated within in the state of California.

261. Lenovo has extensive business connections and disseminates print, video, and Internet advertising to California and from California to other states throughout the United States.

262. Defendant Lenovo represented to Plaintiffs, Class Members, and the general public that the subject computers were reasonably free from significant data security problems.

263. Defendant Lenovo further represented to Plaintiffs, Class Members, and the general public that the subject computers were reasonably fit to access the Internet without exposing personal information or other sensitive data.

264. Specifically, Defendant Lenovo touted the advanced design of the subject computers created by "2000 designers and engineers focused on factors that make a difference to users."[39]

265. Defendant Lenovo marketed the subject computers as safer than other computers due to "built-in security features to help keep your data safer."[40]

266. Defendant Lenovo marketed the subject computers as being able to "ensure total security for your data and identity" with built-in software.[41]

267. While the verbiage of these representations may have varied amongst individual computer lines, the substantive message remained the same: the subject computers are reasonably fit for securely browsing the internet and Lenovo has not

[39] http://shop.lenovo.com/us/en/laptops/lenovo/y-series/y50/#tab-features (last accessed March 4, 2015).

[40] http://shop.lenovo.com/us/en/laptops/lenovo/yoga-laptop-series/yoga-laptop-2-pro/#tab-features (last accessed February 28, 2015).

[41] http://shop.lenovo.com/us/en/laptops/lenovo/yoga-laptop-series/yoga-laptop-2-13/#tab-features (last accessed March 2, 2015).

accepted large amounts of money to pre-install software that hijacks secure communications, steals user information, and insecurely forwards that information to unknown third parties to facilitate unwanted and unauthorized advertising.

268. Defendant Lenovo's statements regarding the quality and/or features of the subject computers were false and served to further the deceptive and fraudulent omissions described above.

269. Defendant Lenovo knew, or would have known through reasonable diligence, its statements regarding the quality and/or features of the subject computers were false.

270. There were reasonably available alternatives to further Defendant Lenovo's legitimate business interests, other than the conduct described herein.

271. On information and belief, Defendant Lenovo has failed to cease its deceptive advertising practices, and has continued to affirmatively make false statements to consumers regarding the subject software, and will continue to do those acts unless this Court orders Defendant to cease and desist pursuant to California Business and Professions Code § 17535.

272. Defendant Lenovo's false, misleading, and deceptive affirmative statements were made in violation of the False Advertising Law, Cal. Bus. & Prof. Code § 17500, et seq.

273. Defendant Lenovo's material omissions were made in violation of the False Advertising Law, Cal. Bus. & Prof. Code § 17500, et seq.

274. Plaintiff Wu and all members of the California Class suffered injuries in fact as a result of Defendant Lenovo's conduct, including out of pocket expenses.

275. As a direct and proximate cause of Defendant Lenovo's false advertising, Plaintiff Wu and the California Class Members incurred the following damages and/or losses:

a. Based on reports of prior and ongoing attacks that exploit the subject software, Plaintiff Wu and other California Class Members incurred economic damages through the purchase of credit monitoring services to mitigate imminent threats of identity theft caused by Defendant Lenovo and verify that their personal data has not already been used for further criminal purposes;

b. Plaintiff Wu and the California Class Members incurred economic damages due to Defendants' misrepresentations and material omissions regarding their data collection and privacy practices, which lured Plaintiff Wu and the California Class Members into spending more money for their computers than they would have had they known of the existence, functionality, and security threat caused by the subject software;

c. The time spent evaluating problems caused by the subject software prior to identifying the software, removing the subject software, evaluating damages caused by the subject software, and remedying damages caused by the subject software resulted in substantial losses of lost time, labor, and goodwill to Plaintiff Wu and the California Class Members; and/or

d. The subject software caused other damages and losses to Plaintiff Wu and the California Class Members by reducing computer and network performance through the unauthorized use of system and networking resources on the subject computers.

276. Pursuant to Business and Professions Code §§ 17203 and 17535, Plaintiff Wu and the California Class seek an order of this Court enjoining Defendant Lenovo from continuing to engage, use, or employ the above-described practices in advertising the sale of the subject computers.

277. Pursuant to Business and Professions Code §§ 17203 and 17535, Plaintiff Wu and the California Class seek an order of this Court requiring

Defendant Lenovo to make full corrective disclosures to correct its prior misrepresentations, omissions, failures to disclose, and partial disclosures.

278. Plaintiff Wu and the California Class seek an order requiring Defendant Lenovo to disgorge itself of all fraudulently obtained gains, and/or be subject to other equitable relief available to Plaintiff. All such remedies are cumulative of relief under other laws, pursuant to California Business & Professions Code § 17205. Additionally, Plaintiffs are entitled to injunctive relief and attorney’s fees as available under California Business and Professions Code § 17200 and other applicable law.

COUNT 13
Defendant Superfish:
Violations of California’s Computer Crime Law

279. Cal. Penal Code § 502, California’s Computer Crime Law (CCCL) prohibits unauthorized access, acquisition, use, or similar behavior with regard to electronic information and data.

280. Defendant Superfish knowingly used the subject software to intercept user data, control and monitor user Internet connections, alter secure communications, and otherwise wrongfully controlled or obtain user data in violation of violation of Cal. Penal Code § 502(c)(1).

281. Defendant Superfish knowingly and without permission accessed, monitored, and seized control of internet communications on the subject computers, transferred user information to Superfish owned and/or operated servers, and otherwise wrongfully made use Plaintiff Wu and other California Class members' data in violation of Cal. Penal Code § 502(c)(2).

282. Defendant Superfish knowingly and without permission used or caused to be used computer services, including but not limited to random access memory (RAM) allocations, hard drive space, and/or networking bandwidth in violation of Cal. Penal Code § 502(c)(3).

283. Defendant Superfish knowingly and without permission injected code into incoming data streams on the subject computers in violation of Cal. Penal Code § 502(c)(4).

284. Defendant Superfish knowingly and without permission intercepted encrypted data users intended to send to a third-party server, decrypted the data through SSL hijacking, re-encrypted the data with an insecure root security

certificate, transmited the data to servers owned and/or operated by Defendant Superfish, and otherwise altered user data in violation of Cal. Penal Code § 502(c)(4).

285. Defendant Superfish knowingly and without permission used the subject software to disrupt usage of the subject computers by a) blocking users from accessing websites that correctly identify the security threat posed by the subject software and b) blocking users from directly accessing websites without first connecting to servers owned and/or operated by Defendant Superfish in violation of Cal. Penal Code § 502(c)(5).

286. Defendant Superfish knowingly and without permission provided, or assisted in providing, a means of accessing user data on the subject computers through its use of an insecure root security certificate in violation of Cal. Penal Code § 502(c)(6).

287. Defendant Superfish knowingly and without permission accessed user data on the subject computers, appropriated the data for its financial gain, and injected unauthorized advertising into data requested by Plaintiffs and other members of California Class in in violation of Cal. Penal Code § 502(c)(7).

288. Defendant Superfish knowingly and without permission introduced a contaminant into the subject computers through its use of an insecure root security certificate in violation of Cal. Penal Code § 502(c)(6).

289. As a direct and proximate cause of Defendant Superfish's violations of the CCCL, Plaintiff Wu and the California Class Members incurred the following damages and/or losses:

a. Based on reports of prior and ongoing attacks that exploit the subject software, Plaintiff Wu and other California Class Members incurred economic damages through the purchase of credit monitoring services to mitigate imminent threats of identity theft caused by Defendant Superfish and verify that their personal data has not already been used for further criminal purposes;

b. Plaintiff Wu and the California Class Members incurred economic damages due to Defendant Superfish's material omissions regarding their data collection and privacy practices, which lured Plaintiff Wu and the California Class Members into spending more money for their computers than they would have had they known of the existence, functionality, and security threat caused by the subject software;

c. The time spent evaluating problems caused by the subject software prior to identifying the software, removing the subject software, evaluating damages caused by the subject software, and remedying damages caused by the subject software resulted in substantial losses of lost time, labor, and goodwill to Plaintiff Wu and the California Class Members; and/or

d. The subject software caused other damages and losses to Plaintiff Wu and the California Class Members by reducing computer and network performance through the unauthorized use of system and networking resources on the subject computers.

290. Plaintiff Wu and the California Class Members have also suffered irreparable injury from these unauthorized acts of disclosure in that their information a) has been harvested, retained, and used by Defendant Superfish, b) which information continues to be retained and may be used by Defendant Superfish and c) due to the continuing threat of such injury and, in addition, the threat that Defendant Superfish will transfer Plaintiffs' and Class Members' information to other third parties, Plaintiffs and Class Members have no adequate remedy at law, entitling them to injunctive relief.

291. Defendants are liable for all statutory, exemplary, and compensatory damages proximately caused and/or flowing from Defendant Superfish's violations of the CCCL, specifically including attorney's fees pursuant to Cal. Penal Code § 502(e).

292. Plaintiffs and the Class Members are entitled to punitive or exemplary damages pursuant to Cal. Penal Code § 502(e)(4) because Defendant Superfish's violations were willful and designed to further a scheme of oppression, fraud, or malice as defined in Cal. Civil Code § 3294.

V. JURY DEMAND

293. Plaintiffs demand a trial by jury for all of their claims at law.

VI. PRAYER FOR RELIEF

WHEREFORE, Plaintiffs and the Class Members request judgment against Defendants, jointly and severally, as follows:

1. An order certifying this action as a class action, appointing Plaintiffs as class representatives and appointing Plaintiffs' counsel as lead Class counsel;

2. All compensatory damages on all applicable claims in an amount to be proven at trial, and, as allowed by law, for such damages to be trebled or multiplied upon proof of claims under laws allowing for trebling or multiplying of compensatory damages based upon Defendants' violations of law;

3. An order directing disgorgement and restitution of all improperly retained monies by Defendants;

4. An order permanently enjoining Defendants from engaging in the unlawful practices, as alleged herein;

5. For an injunction to prohibit Defendants from engaging in the unconscionable commercial practices complained of herein, and for an injunction requiring to give notice to persons to whom restitution is owing of the means by which to file for restitution;

6. For punitive damages against Defendants in an amount to be determined at trial;

7. An award of attorneys' fees, costs, and expenses;

8. All other and further relief, including equitable and injunctive relief, that the Court deems appropriate and just under the circumstances.

[Signatures on following page]

Respectfully submitted this 16th day of March, 2015.

HORMOZDI LAW FIRM, LLC

/s/ Shireen Hormozdi
Shireen Hormozdi
North Carolina Bar No. 47432

1770 Indian Trail Lilburn Road
Suite 175
Norcross, GA 30093
Tel: 800-994-9855
Cell: 678-960-9030
Fax: 866-929-2434
shireen@norcrosslawfirm.com

PRO HAC VICE TO BE FILED FOR:

THE WERNER LAW FIRM, P.C.

/s/ Matthew Q. Wetherington
MATTHEW Q. WETHERINGTON
Georgia Bar No. 339639
ADAM L. HOIPKEMIER
Georgia Bar No. 745811

2142 Vista Dale Court
Atlanta, GA 30084
Phone: (770) VERDICT
Fax: 855-873-2090
matt@wernerlaw.com
adam@wernerlaw.com

Attorneys for Plaintiffs